# SECTION J-2 CONTACT ATTACHMENTS

# ATTACHMENT (10) SECURITY FORM DD254, 16 JANUARY 2002

# DEPARTMENT OF DEFENSE
# CONTRACT SECURITY CLASSIFICATION SPECIFICATION

*(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)*

**1. CLEARANCE AND SAFEGUARDING**

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

**2. THIS SPECIFICATION IS FOR:** *(X and complete as applicable)*

| | | | |
|---|---|---|---|
| X | a. PRIME CONTRACT NUMBER: N00039-02-C-3238 | | |
| | b. SUBCONTRACT NUMBER | | |
| | c. SOLICITATION OR OTHER NUMBER: N00039-01-R-1010 | DUE DATE *(YYYYMMDD)* | |

**3. THIS SPECIFICATION IS:** *(X and complete as applicable)*

| | | | |
|---|---|---|---|
| X | a. ORIGINAL *(Complete date in all cases)* | | DATE *(YYYYMMDD)*: 20021114 |
| | b. REVISED *(Supersedes all previous specs)* | REVISION NO. | DATE *(YYYYMMDD)* |
| | c. FINAL *(Complete Item 5 in all cases)* | | DATE *(YYYYMMDD)* |

**4. IS THIS A FOLLOW-ON CONTRACT?** ☐ YES ☒ NO. If Yes, complete the following:

Classified material received or generated under is transferred to this follow-on contract.

**5. IS THIS A FINAL DD FORM 254?** ☐ YES ☒ NO. If Yes, complete the following:

In response to the contractor's request dated , retention of the classified material is authorized for the period of

**6. CONTRACTOR** *(Include Commercial and Government Entity (CAGE) Code)*

| a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip) |
|---|---|---|
| NORTHROP GRUMMAN INFORMATION TECHNOLOGY, INC.<br>7575 COLSHIRE DRIVE<br>MCLEAN, VA 22102 | 1V4D7 | DEFENSE SECURITY SERVICE<br>7010 LITTLE RIVER TURNPIKE, SUITE #310<br>ANNANDALE, VA 22003 |

**7. SUBCONTRACTOR**

| a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip)* |
|---|---|---|
| | | |

**8. ACTUAL PERFORMANCE**

| a. LOCATION | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip)* |
|---|---|---|
| | | |

**9. GENERAL IDENTIFICATION OF THIS PROCUREMENT**

DEFENSE INTEGRATED MILITARY HUMAN RESOURCE SYSTEMS (DIMHRS)

| 10. CONTRACTOR WILL REQUIRE ACCESS TO: | YES | NO | 11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: | YES | NO |
|---|---|---|---|---|---|
| a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION | | X | a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY | | X |
| b. RESTRICTED DATA | | X | b. RECEIVE CLASSIFIED DOCUMENTS ONLY | | X |
| c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION | | X | c. RECEIVE AND GENERATE CLASSIFIED MATERIAL | X | |
| d. FORMERLY RESTRICTED DATA | | X | d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE | | X |
| e. INTELLIGENCE INFORMATION: | | | e. PERFORM SERVICES ONLY | | X |
| (1) Sensitive Compartmented Information (SCI) | | X | f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES | | X |
| (2) Non-SCI | | X | g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER | X | |
| f. SPECIAL ACCESS INFORMATION | | X | h. REQUIRE A COMSEC ACCOUNT | | X |
| g. NATO INFORMATION | | X | i. HAVE TEMPEST REQUIREMENTS | X | |
| h. FOREIGN GOVERNMENT INFORMATION | | X | j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS | | X |
| i. LIMITED DISSEMINATION INFORMATION | | X | k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE | | X |
| j. FOR OFFICIAL USE ONLY INFORMATION | X | | l. OTHER (Specify | | X |
| k. OTHER (Specify)<br><br>PR NO.: | | X | | | |

**12. PUBLIC RELEASE.** Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through *(Specify):*

COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND, CODE 00L, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127 to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.

* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

**13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

**CLASSIFICATION GUIDES: (PROVIDED UNDER SEPARATE COVER BY SPAWAR IT CENTER, NEW ORLEANS, REFER TO CONTACT INFORMATION BELOW )**

OPNAVINST S5513.6C, ENCL (4), SECURE VOICE INTEROPERAVILITY SYSTEM (SVIS)
OPNAVINST S5513.6C, ENCL (5), MULTI-USER SPECIAL INTELLIGENCE COMMUNICATION TACTICAL INTELLIGENCE
OPNAVINST S5513.6C, ENCL (6), CIRCUIT MAYFLOWER
OPNAVINST S5513.6C, ENCL (7), CLARINET MERLIN
OPNAVINST S5513.6C, ENCL (8), COMPACT VERY LOW FREQUENCY (CVLF)
OPNAVINST S5513.6C, ENCL (11), STRATEGIC COMMAND AND CONTROL COMMUNICATIONS SYSTEM

**(*ADDITIONAL CLASSIFICATION GUIDES CONTINUED - NEXT PAGE*)**

**ACCESS REQUIREMENTS:**

**11C**. A GSA APPROVED CONTAINER IS REQUIRED.

**11.G** THE CONTRACTOR IS AUTHORIZED THE USE OF DTIC REGARDING **SPECIFIC CONTRACT RELATED INFORMATION** AND WILL PREPARE AND PROCESS DD FORM 1540 IN ACCORDANCE WITH THE NISPOM, CHAPTER 11, SECTION 2. THE COR WILL CERTIFY NEED-TO-KNOW TO DTIC.

**NORTHROP GRUMMAN INFO. TECH, INC. (CAGE CODE: 1V4D7) CLASSIFIED MAILING ADDRESS:**
**NORTHROP GRUMMAN INFORMATION TECHNOLOGY, INC.**
**7575 COLSHIRE DRIVE**
**MAILSTOP C1W4**
**MCLEAN, VA 22102**

**SPAWAR-IT CENTER CONTRACTING OFFICER REPRESENTATIVE (COR)/TASK MANAGER: MR. ROBERT CASTRO, PROGRAM OPERATIONS OFFICER, SPAWAR INFORMATION TECHNOLOGY (IT) CENTER, 2251 LAKESHORE DRIVE, NEW ORLEANS, LA, 70145, PHONE: (504) 697-3505.**

**ALL CLASSIFIED INFORMATION MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 12958-CLASSIFIED NATIONAL SECURITY INFORMATION, OF 17 APRIL 1995. YOUR DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY REPRESENTATIVE (IS REP) SHOULD BE CONTACTED FOR ASSISTANCE.**

COPIES OF ALL SUBCONTRACT DD FORM 254S MUST BE PROVIDED TO THE DISTRIBUTION LISTED IN BLOCK 17.

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. ☒ YES ☐ NO

*(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)*

***(SOME SECURITY REQUIREMENTS ARE SITE SPECIFIC – CONTACT LOCAL SECURITY OFFICE FOR THEIR SECURITY REQUIREMENTS FOR ON-SITE)***

SPECIFIC ON-SITE SECURITY REQUIREMENTS ATTACHED.
INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY REQUIREMENTS ATTACHED AND MUST BE PROVIDED TO ALL SUBCONTRACTORS.
FOR OFFICIAL USE ONLY (FOUO) INFORMATION REQUIREMENTS ATTACHED.
CONTRACTOR TEMPEST REQUIREMENTS ATTACHED AND MAY BE PASSED TO SUBCONTRACTORS.

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ YES ☒ NO

*(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)*

**16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.**

| a. TYPED NAME OF CERTIFYING OFFICIAL | b. TITLE | c. TELEPHONE *(Include Area Code)* |
|---|---|---|
| SUE.VILLARREAL@NAVY.MIL<br>SUSAN VILLARREAL | SECURITY'S CONTRACTING OFFICER'S REPRESENTATIVE | (619) 524-2672 |

d. ADDRESS *(Include Zip Code)*
COMMANDING OFFICER
SPAWAR SYSTEMS CENTER CODE 20351
53560 HULL ST.
SAN DIEGO, CA 92152-5001

e. SIGNATURE
20021114 Susan M. Villarreal

**17. REQUIRED DISTRIBUTION**
☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY SSC -SD 20351,SPAWAR -ITC New Orleans

**BLOCK 13 CLASSIFICATION GUIDES CONTINUED……**

OPNAVINST S5513.6C, ENCL (19) SHF SATELLITE COMMUNICATIONS TERMINALS (SHIPBOARD)
OPNAVINST S5513.6C, ENCL (22) SSN INTEGRATED COMMUNICATIONS SYSTEM
OPNAVINST S5513.6C, ENCL (29) DIRECTION FINDING SWITCHING UNIT
OPNAVINST S5513.6C, ENCL (32) GEODETIC SATELLITE (GEOSAT-A)
OPNAVINST S5513.6C, ENCL (41) TACINTEL II
OPNAVINST S5513.6C, ENCL (42) TACTICAL DATA INFORMATION EXCHANGE SYSTEM (TADIXS)-B TACTICAL RECEIVE EQUIPMENT (TRE)
OPNAVINST S5513.6C, ENCL (44) DIGITAL WIDEBAND TRANSMISSION SYSTEM (DWTS), LINE-OF-SIGHT RADIO SYSTEM (LRS)
OPNAVINST S5513.8B, ENCL (3) ECM/ECCM, GENERAL
OPNAVINST S5513.8B, ENCL (4) ELECTRO-OPTICS SENSOR
OPNAVINST S5513.8B, ENCL (5) ELINT, GENERAL
OPNAVINST S5513.8B, ENCL (9) HULL-TO-EMITTER CORRELATION (HULTEC)
OPNAVINST S5513.8B, ENCL (11) LASER GUIDANCE SYSTEMS
OPNAVINST S5513.8B, ENCL (13) MINIATURE EXPENDABLE JAMMERS
OPNAVINST S5513.8B, ENCL (14) OPERATIONAL ELECTRONIC WARFARE AND FLEET ELECTRONIC WARFARE SUPPORT GROUP (FEWSG) OPERATIONS
OPNAVINST S5513.8B, ENCL (16) OUTBOARD/OUTBOARD II
OPNAVINST S5513.8B, ENCL (17) OVER-THE-HORIZON TRAGETING
OPNAVINST S5513.8B, ENCL (18) RADAR, GENERAL
OPNAVINST S5513.8B, ENCL (20) RECEIVER SYSTEM AN/WLR-8(V)
OPNAVINST S5513.8B, ENCL (21) AN/WLQ-4(V), SEA NYMPH
OPNAVINST S5513.8B, ENCL (30) (AN/SLQ-34 ELECTRONIC COUNTERMEASURES SET; AN/SLR-22 COUNTERMEASURES RECEIVING SET
OPNAVINST S5513.8B, ENCL (31) COUNTERMEASURES SET, AN/ALQ-165, AIRBORNE SELF-PROTECTION JAMMER (ASPJ)
OPNAVINST S5513.8B, ENCL (33) SIGNAL DETECTION AND DIRECTION FINDING SRS-1 (XN-1) SYSTEM
OPNAVINST S5513.8B, ENCL (35) RADAR (SAR), SYNTHETIC APERTURE
OPNAVINST S5513.8B, ENCL (36) ECCM RADIO, AN/ARC—182(V)
OPNAVINST S5513.8B, ENCL (37) RADAR EMITTER CLASSIFICATION AND IDENTIFICATION (RECI)
OPNAVINST S5513.8B, ENCL (38) AN/SLQ-32(V)1,(V)2 , (V) 3
OPNAVINST S5513.8B, ENCL (40) OSIS BASELINE UPGRADE (OBU)
OPNAVINST S5513.8B, ENCL (43) TARGETING AVIONICS TECHNOLOGY
OPNAVINST S5513.8B, ENCL (44) BATTLE GROUP PASSIVE HORIZON EXTENSION SYSTEM (BGPHES)
OPNAVINST S5513.8B, ENCL (45) RELOCATION OVER-THE-HORIZON RADAR (ROTH-R)
OPNAVINST S5513.8B, ENCL (46) MOBILE ELECTRONIC WARFARE SUPPORT SYSTEM (MEWSS)
OPNAVINST S5513.8B, ENCL (48) AFLOAT CORRELATION SYSTEM (ACS)
OPNAVINST S5513.8B, ENCL (50) INTEGRATED SIGNALS INTELLIGENCE SYSTEM (ISIS)
OPNAVINST S5513.8B, ENCL (51) AN/SLQ-17A(V)2
OPNAVINST S5513.8B, ENCL (53) AN/WLR-1H
OPNAVINST S5513.8B, ENCL (55) ELECTRONIC INTELLIGENCE SUPPORT SYSTEM (ESS)
OPNAVINST S5513.8B, ENCL (56) WIDEBAND SYSTEM (WBS) (AN/FSQ-/117A(V))
OPNAVINST S5513.8B, ENCL (58) NULKA (FORMERLY SHIP-LANUNCHED ELECTRONIC DECOY
OPNAVINST S5513.8B, ENCL (63) AN/SLQ-49, INFLATABLE DECOY
OPNAVINST S5513.8B, ENCL (64) AN/SLQ-39, CHAFF BUOY
OPNAVINST S5513.8B, ENCL (65) AN/SSQ-95, ACTIVE ELECTRONIC BUOY (AEB)
OPNAVINST S2221, RELEASE OF COMMUNICATION SECURITY (COMSEC) MATERIAL TO US INDUSTRIAL FIRMS UNDER CONTRACT TO THE US NAVY
OPNAVINST S3432.1, OPERATION SECURITY

## INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS

The U.S. Government conducts trustworthiness investigations of personnel who require access to only unclassified information and who perform IT duties. Requirements for these investigations are outlined in paragraphs 3-614, 3-710 and Appendix K of DoD 5200.2-R, available at http://www.ntis.gov. (Search site: PB2002-107366). Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories below. The contractor shall include all of these requirements in any subcontracts involving IT support.

DoD 5200.28 (Security Requirements for Automated Information Systems (AIS)), paragraph 4.10 which states "Access by foreign nationals to a US government-owned or US Government-managed AIS may be authorized only by the DOD Component Head, and shall be consistent with the DOD, Department of State, and the Director of Central Intelligence policies." The DoD Component Head for the Department of the Navy is the Secretary of the Navy (SECNAV). SECNAV approval is required for all IT access by non-U.S. citizens.

The Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the IT Position category to contractor personnel and inform the contractor of their determination. If it is decided the contractor shall make the assignment, the COR or TR must concur with the designation.

**IT-I Position (High Risk)** – Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years.

**IT-II Position (Moderate Risk)** - Positions in which the incumbent is responsible for the direction, planning, design, operation or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check (NAC).

**IT-III Position (Low Risk)** - All other positions involving IT activities. Incumbent in this position has non-privileged access to one or more DoD information systems/application or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated NAC.

If an employee has a personnel security investigation at the appropriate level without a break in service for more than 24 months, with favorable adjudication, and in the case of IT-I Position is less than 5 years old, you do **not** need to submit an additional investigation for the trustworthiness determination. If required, the contractor will ensure personnel designated IT-I, II, or III complete the Standard Form (SF) 85P. The company shall review the SF 85P for completeness and use Appendix G, SECNAVINST 5510.30A to determine if any adverse information is present. The reviewer shall submit the SF85P to SPAWARSYSCEN San Diego, Code 20351, 53560 Hull Street, San Diego, CA 92152-5001. **Only** hard copy SF85Ps are acceptable. An employee may not begin work on IT equipment until the company receives written notification from Code 20351. For additional assistance please send email to SF85P@spawar.navy.mil.

Specific guidelines for obtaining software of the SF85P are available at http://www.dss.mil. If you are unfamiliar with the SF85P, you may send email to SF85P@spawar.navy.mil.

Investigation results shall be returned to SPAWARSYSCEN San Diego, Code 20351, 53560 Hull Street, San Diego, CA 92152-5001 for a trustworthiness determination. SPAWARSYSCEN San Diego will notify the contractor of its decision. The contractor will promptly replace any individual for whom SPAWARSYSCEN San Diego has communicated a negative trustworthiness determination.

The contractor will include the IT Position Category for each person so designated on Visit Authorization Letters (VAL) once the COR or TR has approved the Category and written notification from Code 20351 has been received. VALs will be sent to the

following address: Commanding Officer, SPAWARSYSCEN San Diego, ATTN: Code 20352, 49275 Electron Drive, San Diego, CA 92152-5435.

**SPECIFIC ON-SITE SECURITY REQUIREMENTS**

I. GENERAL.

a. Contractor Performance. In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD 254. The Contractor will conform with the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM) available from www.dss.mil. When visiting COMSPAWARSCOM at either Old Town Campus (OTC) or Point Loma Campus (PLC) the Contractor will comply with the security directives used regarding the protection of classified and sensitive but unclassified (SBU) information, SECNAVINST 5510.36 (series) and SECNAVINST 5510.30 (series) both of which are available from http://neds.nebt.daps.mil/Directives/table52.html. A hardcopy of these directives will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SPAWAR Systems Command's Security Contracting Officer's Representative (COR), Code 20351. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at COMSPAWARSYSCOM, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWAR Systems Center will exercise security supervision over all contractors visiting COMSPAWARSYSCOM and will provide security support to the Contractor as noted below. The Contractor will identify, in writing to Security's COR, an on-site Point of Contact to interface with Security's COR.

II. HANDLING CLASSIFIED MATERIAL OR INFORMATION.

a. Control and Safeguarding. Contractor personnel located at COMSPAWARSYSCOM are responsible for the control and safeguarding of all classified material in their possession. All contractor personnel will be briefed by their FSO on their individual responsibilities to safeguard classified material. In addition, all contractor personnel are invited to attend SPAWAR Systems Center conducted Security Briefings, available at this time by appointment only. In the event of possible or actual loss or compromise of classified material, the on-site Contractor at the PLC will immediately report the incident to SPAWAR Systems Center's Code 20351 as well as the Contractor's FSO. An on-site Contractor, whose primary location is OTC, will make their report to Code 20351 as well as the Contractor's FSO. A Code 20351, representative will investigate the circumstances, determine culpability where possible and report results of the inquiry to the FSO and the Cognizant Field Office of the DSS. On-site contractor personnel will promptly correct any deficient security conditions identified by a SPAWAR Systems Center Security representative.

b. Storage.

1. Classified material may be stored in containers authorized by SPAWAR Systems Center's PLC Physical Security Group, Code 20352, or OTC Code 20351, for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board COMSPAWARSYSCOM with Code 20352's written permission. Containers to be located at our OTC will request Code 20351's written permission. Areas located within cleared contractor facilities at COMSPAWARSYSCOM will be approved by DSS.

2. The use of Open Storage areas must be pre-approved in writing by SPAWAR Systems Center, Code 20352, for the open storage, or processing, of classified material prior to use of that area for open storage. Specific supplemental security controls for open storage areas, when required, will be provided by SPAWAR Systems Center, Code 20352.

c. Transmission of Classified Material.

1. All classified material transmitted by mail for use by long term visitors will be addressed to COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, 53560 HULL ST, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their Code number.

2. All SECRET material hand carried to COMSPAWARSYSCOM by contractor personnel must be delivered to the SPAWAR Systems Center Classified Material Control Center (CMCC), Code 20332, for processing.

3. All CONFIDENTIAL material hand carried to COMSPAWARSYSCOM by contractor personnel must be delivered to the Mail Distribution Center, Code 20331, for processing. This applies for either the OTC or PLC sites.

4. All COMSPAWARSYSCOM classified material transmitted by contractor personnel from COMSPAWARSYSCOM will be sent via the COMSPAWARSYSCOM COR or TR for this contract.

5. The sole exception to the above are items categorized as a Data Deliverable. All contract Data Deliverables will be addressed to COMMANDER, ATTN RECEIVING OFFICER CODE 2242, SPAWAR SYSTEMS COMMAND, 4201 PACIFIC HIGHWAY, SAN DIEGO, CA 92110-3127.

III. INFORMATION ASSURANCE (IA) SECURITY. Contractors using Information Systems, networks or computer resources to process classified, SBU or unclassified information will comply with the provisions of SECNAVINST 5239.3 (series) available at: http://neds.nebt.daps.mil/Directives/table48.html and local policies and procedures. Contractor personnel must ensure that systems they use at COMSPAWARSYSCOM have been granted a formal letter of approval to operate by contacting their Information System Security Officer (ISSO). A list of ISSOs is available from https://iweb.spawar.navy.mil/services/security/docs/Issolist.htm.

IV. VISITOR CONTROL PROCEDURES.

a. Contractor personnel assigned to COMSPAWARSYSCOM will be considered long-term visitors for the purpose of this contract.

b. Submission of valid Visit Authorization Letter (VAL) for classified access to COMSPAWARSYSCOM is the responsibility of the Contractor's Security Office. All VAL's will be prepared in accordance with the NISPOM. They will be sent to either COMMANDING OFFICER, ATTN CODE 20352, SPAWAR SYSTEMS CENTER, 49275 ELECTRON DRIVE, SAN DIEGO, CA 92152-5435 for the PLC, or COMMANDING OFFICER, VISITOR CONTROL OTC, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO, CA 92152-5001 for OTC. The VAL's will be addressed to COMSPAWARSYSCOM and list a COMSPAWARSYSCOM point of contract. Visit requests may be sent via facsimile to the PLC at (619) 553-6169, and verified on(619) 553-3203 or the OTC at (619) 524-2745, and verified on (619) 524-2751 or 524-3124.

c. Visit requests for long-term visitors should be received at least one week prior to the expected arrival of the visitor to ensure necessary processing of the request.

d. Code 20352 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible COMSPAWARSYSCOM COR will request issuance of picture badges to contractor personnel. The COR may, at their discretion, request that picture badges be issued for the length of the basic contract or option period. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of a COMSPAWARSYSCOM badge will be reported to the DSS. Identification badges must be worn in plain sight at all times on board COMSPAWARSYSCOM.

e. Prior to the termination of a Contractor employee with a COMSPAWARSYSCOM badge or active VAL on file the FSO must:

1. Notify in writing Code 20352 for PLC, Code 20351 for OTC, the COR, Security's COR, and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the termination and effective date. In emergency situations, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.

2. Confiscate any COMSPAWARSYSCOM identification badge and vehicle decal and return them to either Code 20352, or Code 20351, no later than 5 working days after the effective date of the termination.

V. INSPECTIONS. Code 20351 personnel will conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel shall cooperate with Code 20351 representatives during these inspections. A report of the inspection will be forwarded to the Contractor's employing facility and COR. The Contractor must be responsive to the Code 20351 representative's findings.

VI. REPORTS. As required by the NISPOM, Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication classified information has been lost or compromised. The Contractor shall ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 20351. This reporting will include the following:

a. The denial, suspension or revocation of security clearance of any assigned personnel;

b. Any adverse information that would cast doubt on an assigned employee's continued suitability for continued access to classified access;

c. Any instance of loss or compromise, or suspected loss or compromise, of classified information;

d. Actual, probable or possible espionage, sabotage, or subversive information; or

e. Any other circumstances of a security nature that would effect the contractor's operation on board COMSPAWARSYSCOM

VII. PHYSICAL SECURITY.

a. SPAWAR Systems Center will provide appropriate response to emergencies occurring onboard this command. The Contractor will comply with all emergency rules and procedures established for COMSPAWARSYSCOM.

b. A roving Contract Security Guard patrol will be accomplished by SPAWAR Systems Center. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to either PLC Code 20352 or OTC Code 20351.

c. All personnel aboard COMSPAWARSYSCOM AND SPAWAR Systems Center are subject to random inspections of their vehicles, personal items and of them selves. Consent to these inspections is considered to have been given when personnel accept either a badge or a vehicle pass or decal permitting entrance to the command.

VIII. COR RESPONSIBILITIES.

a. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions and/or submits a Final DD 254 to Security's COR.

b. Coordinates, in conjunction with the appropriate transportation element, a suitable method of shipment for classified material when required.

c. Certifies and approves Registration For Scientific and Technical Information Services (DTIC) requests (DD 1540).

d. Ensures that timely notice of contract award is given to host commands when contractor performance is required at other locations.

e. Certify need-to-know on visit requests, conference registration forms, etc.

IX. SECURITY'S COR RESPONSIBILITIES.

a. Initiate all requests for facility clearance action for our prime contractors with the DSS.

b. Validate justification for Interim Top Secret personnel security clearances and facility clearances.

c. Validate and endorse requests submitted by a cleared contractor for Limited Access Authorizations (LAA) for its non-U.S. citizen employees.

X. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

Any cleared contractor facility on board SPAWARSYSCOM will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional COMSPAWARSYSCOM contracts may be authorized to use this cleared facility, but only on a case-by-case basis. The COR, Security's COR, and Contracting Officer must be in agreement that this particular arrangement best suits the needs of the Government. At the end of this contract the on-site facility must be vacated, with proper written notification being submitted to the DSS and Security's COR.

XI. ITEMS PROHIBITED ABOARD COMSPAWARSYSCOM/SPAWAR Systems Center.

a. Dangerous weapon, instrument or device includes, but is not limited to, the following:

rifles, automatic rifles, machine guns, sub-machine guns, pistols, machine pistols, flare pistols, starter pistols, shotguns, compressed gas, air or spring fired pellet or "BB" guns, sling shots, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projective or other device which may injure someone;

daggers, switch blades, bow and arrows, sear guns, Hawaiian slings, power heads, fishing knives, scuba knives, or any unofficial knife with a blade longer than 2 1/2 inches;

martial arts devices (throwing stars, nunchakus), stun guns, tasers, brass knuckles, billy clubs, night sticks, pipe, bars, or mallets, or other similar devices capable of being used as a weapon;

poison, acids or caustic chemicals;

or any other item that may be used to inflict serious injury or death to another person or temporarily blind or disable an individual injury not specifically authorized by proper authority.

b. Explosive article or compound includes but is not limited to: ammunition for any of the small arms weapons mentioned as a dangerous weapon, including "blank" ammunition, gunpowder, molotov cocktails, pipe bombs, grenades, pyrotechnics, fireworks or any other compound or article which might violently react and cause injury not specifically authorized by proper authority.

c. As an exception to the list of dangerous weapons, the possession of defensive tear gas devices (e.g., pepper spray) aboard all naval installations in California is now permissible. However, unauthorized use of these devices other than for self-defense will be prosecuted as a violation of the Uniform Code of Military Justice or applicable laws.

XII. ESCORTING POLICY.

a. All personnel within COMSPAWARSYSCOM/SPAWAR Systems Center's fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear a SPAWAR Systems Center issued badge. The words "Security" or "Safety" on selective Code 2031 or 2038 employee badges authorizes the bearer to escort unbadged emergency vehicles and operators and support personnel during emergencies. Only U.S. citizens and intending citizens (former immigrant aliens) may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SPAWAR SYSTEMS COMMAND FOREIGN DISCLOSURE OFFICE, 08-42.

b. All permanently badged COMSPAWARSYSCOM/SPAWAR Systems Center and tenant command employees, as well as those contractors and other government employees who have an "E" for escort on their permanent badges may escort visitors requiring escort.

XIII. CONTRACTOR TRAINING.

All contractor personnel cleared Top Secret, Secret, or Confidential are required to receive annual Security Training. The issuance of a picture badge will trigger an e-mail to be sent to your personnel. This e-mail will give your employee the site of the computer-based training that must be completed. This training is required to be repeated annually.

**TEMPEST REQUIREMENTS QUESTIONNAIRE**
**FOR CONTRACTOR FACILITIES**

1. This TEMPEST Requirements Questionnaire (TRQ) must be completed and sent to the contracting authority and the Certified TEMPEST Technical Authority (CTTA) within 30 days after contract award for all contracts where classified National Security Information (NSI) will be processed and the requirements of item 13 of the DD 254 have been met.

2. The prime contractor cannot pass TEMPEST requirements to subcontractors. Subcontractors must submit a Contractor TRQ prior to processing.

3. The TRQ is for information collection only. It is not a directive or an implied requirement, nor is it an encouragement to procure TEMPEST equipment or any type of shielding for use on this contract. Do not initiate any changes to equipment of facilities for TEMPEST unless it has been recommended by the CTTA and specifically directed by the contracting authority.

4. The contracting authority will not issue any directives concerning TEMPEST until after the contractor submitted TRQ has been evaluated by the CTTA and resulting recommendations received. To fully evaluate the TRQ, the CTTA may request additional information concerning the facility, its physical control, the equipment which will be used to process NSI, etc.

5. The contractor shall ensure compliance with any TEMPEST countermeasure(s) specifically directed in writing by the contracting authority.

6. Please provide the information requested in paragraphs 7 through 20 and return to the CTTA at:

Commanding Officer
SPAWARSYSCEN Charleston
Code 723
PO Box 190022
North Charleston, SC 29419-9022

7. Provide the name, address, position title and phone number (at the facility where classified processing will occur) of a point of contact who is knowledgeable of the processing requirements, the types of equipment to be used and the physical layout of the facility.

8. Provide the specific geographical location, address, and zip code, where classified processing will be performed.

9. What are the classification level(s) of material to be processed/handled by electronic or electromechanical information system(s) and what percentage is processed at each level?

10. What special categories of classified information are processed?

11. Is there a direct connection (wire line or fiber) to a Radio Frequency (RF) transmitter(s) located either locally or at a remote site?

12. Are there any RF transmitters located within 6 meters of the system processing National Security Information or the system's RED signal lines?

13. Describe how access is controlled to your facility including the building, compound, plant, property, and/or parking lots. Where are visitor's first challenged/identified? Include controls such as alarms, guards, patrols, fences and

warning signs. Provide a simple block diagram of the equipment, the facility and the surrounding areas. The diagram(s) should extend out to the nearest uncontrolled area on each side of the facility, such as a military base perimeter, plant property line, commercial building or residential area.

14. Are there other tenants in the building who are not U.S. department/agencies or their agents?

15. Are there any known foreign business or government offices in adjacent buildings?

16. Provide the make and model number of all equipment used to process, transfer or store classified information. Include computers, peripherals, network servers, network hardware, multiplexers, modems, encryption devices (COMSEC), etc.

17. Have on-site TEMPEST tests been conducted on any of these equipment(s)? If so, which ones? When was the test(s) conducted? Who conducted the test(s)? Have all deficiencies (if any) been resolved?

18. Has a TEMPEST Facility Zoning test been conducted? If so, who conducted the testing and when?

19. Is this company foreign-owned or controlled? If so, what is the country?

20. Provide the name, code, telephone number, and address of the Contracting Officer's Representative, the contract number and the sponsoring command.

## FOR OFFICIAL USE ONLY (FOUO) INFORMATION

1. The For Official Use Only (FOUO) marking is assigned to information at the time of its creation. It isn't authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).

2. Use of FOUO markings doesn't mean that the information can't be released to the public, only that it must be reviewed by SPAWAR Systems Center San Diego CA prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

3. An UNCLASSIFIED document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the bottom face and interior pages.

4. Classified documents containing FOUO do not require any markings on the face of the document; however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY." Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion.

5. Any FOUO information released to you by SPAWAR Systems Center San Diego CA is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTION(S) _____ APPLY.

6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM SPAWAR SYSTEMS CENTER SAN DIEGO CA OR THE AUTHOR. When the FOUO status is terminated you will be notified.

7. You may disseminate FOUO information to your employees and subcontractors who have a need for the information in connection with this contract.

8. During working hours FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

9. FOUO information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.

10. When no longer needed, FOUO information may be disposed by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash, or recycle, container or in the uncontrolled burn.

11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.